CASE STUDY HEALTHCARE

Denver Health Saves 100+ Hours of In-House Security Analyst Time Per Month With Red Canary

CHALLENGE

Security managers struggled to keep pace with potential threats identified by their EDR product.

REQUIREMENTS

Denver Health needed a resource with deep expertise in EDR to cut through the noise and pinpoint the threats that required action.

SOLUTION

Red Canary's Managed Endpoint Detection and Response (MEDR) identifies true threats and eliminates false positives, giving the hospital security staff peace of mind that they can quickly respond to critical events before they cause damage.

SNAPSHOT

Denver Health is one of Colorado's premier healthcare institutions and home to the region's Level 1 Trauma Center. The hospital had implemented Endpoint Detection and Response (EDR) to get better visibility into its endpoints and defend against evolving threats. But the hospital's security team quickly realized they didn't have the resources or time to keep up with the massive volume of endpoint data and distinguish between EDR alerts and actual threats. Red Canary's managed solution now gives them confidence that endpoint threats will be quickly detected and addressed.

CUT THROUGH THE NOISE

The hospital benefits from Red Canary's dedicated team of expert analysts who define detection criteria and triage and investigate every potential threat. Red Canary's reporting gives the hospital visibility into the threats that require action while reassuring them that no important threats are being missed. Daily EDR management workload has been reduced from hours to minutes, which allows the team to focus on other aspects of its security posture.

TYPICAL 30-DAY PERFORMANCE

58M	processes and executables analyzed across 4,387 endpoints
1,724	potentially threatening events investigated and 37 confirmed threats detected
100+	hours of in-house analysis saved

red canary

> “Red Canary has taken what used to be a daily workload of hours, and brought it down to minutes. Every detection is now actionable and reliable. It has significantly boosted our confidence in our defense posture.”
>
> **— Aaron Post, Security Analyst**

DIGGING DEEPER

A Deluge of False Positives

Keenly aware of the limitations of signature-based antivirus products, the security team turned to EDR to gain visibility into endpoint activity and defend against threats that slipped past its prevention products. Once the EDR product was adopted, the analyst team was inundated with 100,000+ alerts and binaries that needed attention. The continued influx of new alerts and binaries became very challenging to triage and the analyst team was only able to devote time to a limited number of endpoints. It was apparent that managing EDR, alongside all the team’s other daily operational tasks, would be extremely difficult and left uncertainty in effectively catching threats.

An Outsourced Solution

Because the security team was unable to add headcount to keep up with the workload, it decided to outsource. Red Canary enabled Denver Health to take advantage of a dedicated Security Operations Center with extensive EDR expertise. The Red Canary team brought the deep understanding necessary to look at the endpoint data, triage and investigate it, and pass along only what required attention.

Red Canary Delivers Confidence

With Red Canary on hand to evaluate potential threats, the in-house security staff is confident that critical events will be captured immediately. They no longer spend time sorting through false positives and when important issues do arise they can resolve them faster. Additional benefits include:

- Greater overall visibility for network management. For example, IT is now notified when laptops leave the environment or users attempt to install software that was not part of the standard machine image.
- The ability to detect applications and binaries that, while not inherently malicious, have no place in the corporate environment.
- Accurate and actionable detection of threats in the environment.

Iain Lumsden, Information Security Manager, said: “I’m confident in our EDR deployment and the process we have with Red Canary. If Red Canary went away, I’d worry that we wouldn’t catch an event in time that could be disastrous for our environment. I sleep more soundly knowing our environment is in good hands with Red Canary.”